REQUEST FOR CLASSIFIED COMPUTER/NETWORK ACCESS

For use of this form, see AR 25-2

1. NAME (Last, First, MI):	2. ORGANIZATION AND OFFICE SYMBOL:	3. PHONE NUMBER (DSN):

4. GRADE/RANK/CONTRACTOR:	5. DUTY POSITION:	6. VISIT REQUEST ON FILE (Contractor Only): ☐ Yes ☐ No:	7. DATE OF VISIT REQUEST:

8. CLEARANCE: a. Clearance Level:	b. Investigation Type:	c. Date Completed:	d. Submitted By (IASO/Security Manager):	e. IASO/Security Manager Phone No:

9. PRIVILEGED USE (DOIM Use Only): a. Administrator: ☐ Yes ☐ No: b. User: ☐ Yes ☐ No:

10. INITIAL BRIEFING/PASSWORD:

a. Access to a classified computer and/or network is a privilege based upon your duty requirements and trust the Government has in your integrity. You have been authorized access to classified information, the unauthorized disclosure of which could cause damage to national security. You are reminded of your personal, moral, and legal responsibility to protect classified information within your knowledge, possession, or control. Protection of classified information is serious business. We must be alert to violations of good security practices and know procedures for reporting or correcting such violations. Unauthorized disclosure of classified defense information, whether public or private, intentional or unintentional, is subject to prosecution under Section 793 of Title 18, U.S.C., imprisonment, and/or a $10,000 fine, for each count. Additionally, other violations may be punished by letters of reprimand or other administrative punishment, which could be detrimental to your career. In the case of military personnel, UCMJ action is always a possibility for willful violations.

b. AR 380-5 is the basic regulation governing the protection of classified material, and AR 25-2 governs system security. Users of classified information are responsible for safeguarding it. Computer systems that are approved and process classified information must be protected in the same manner as classified "paper" documents.

c. Passwords for classified systems, e-mail accounts, and/or networks are classified at the highest classification level of the system.

d. All media (diskettes, ZIP disks, recordable CD-ROMs, etc.,) introduced into a classified system is considered classified at the highest classification level of the system. The media must be labeled, secured, and destroyed per procedures for classified media.

e. Classified systems are approved under strict configuration guidelines. Users are prohibited from making any changes to system settings, installing software applications or utilities, or modifying/changing system hardware.

f. Your Security Manager/Assistant Security Manager and/or Information Assurance Security Officer are the points of contact for all security matters within your organization. Know who they are. Any questions should be referred to them. If they don't know the answer, they will know who to contact.

g. Access to Government information services constitutes consent to monitoring.

11. ACKNOWLEDGEMENT:

a. I will contact my Security Manager or Information Assurance Security Officer (IASO) for guidance when in doubt about security for any network or system activity I desire to perform and will report any security violations.

b. I am responsible for the protection of this User ID and Password and for any activity that occurs as a result of neglect or intent on my part.

c. I have been briefed and understand my responsibilities as they pertain to the use of a classified computer system/network. I acknowledge that I may be subject to administrative sanctions or action under the UCMJ or Federal Law for violations of security policy and/or procedures.

12. USER NAME (Typed or Printed):	13. SIGNATURE:	14. DATE: